

Hyper-V Practices

By Hyper-V
Virtualization Team

Security

▶ HARDENING AND PROTECTING THE HOST

- *Use Server Core when practical*
 - Ensure you have sufficient staff expertise
 - Beware potential driver problems
- *Run only the Hyper-V role on the host server*
 - Shut down any unnecessary services on the host server
 - Plug and play
 - All other non-essential services
- *Use the Windows Server® 2008 Security Compliance Management Toolkit*
 - The Windows Server 2008 Security Compliance Management Toolkit provides you with an end-to-end solution to help you plan, deploy, and monitor the security baselines of servers running Windows Server® 2008 in your environment.
- *Use discrete NICs for management of host vs. operation of virtual machines*
- *Each Host needs its own firewall, antivirus, and intrusion detection software*
 - *Insert comment here*
- *Host machines should be added to the appropriate organizational units (OUs) so that Group Policy settings apply correctly.*

Security – Cont.

▶ PROTECTING VIRTUAL MACHINES

- *Use Offline Virtual Machines Servicing Tool*
- *Use private or internal network to prevent test virtual machines from access other network resources*
- *Use BitLocker™ Drive Encryption on the Hyper-V host*
 - Prevents worries and potentially expensive reporting requirements in the event that virtual machines are stolen or improperly accessed.
- *Limit physical administrative access to Host servers*
 - Maintain a clear separation between those administrators who are responsible for the operation of the physical server and the management operating system, and those administrators who are responsible for managing individual virtual machines.
 - You can use Authorization Manager (AzMan), a snap-in for the Microsoft® Management Console (MMC), to assign selected users and groups to the Hyper-V Administrator role so they can use Hyper-V Manager without being administrators of the physical computer itself.

Audit access to all virtual machines

- Virtual machines access should be audited just like physical servers

Security – Cont.

▶ DELEGATING VIRTUAL MACHINE MANAGEMENT (SCVMM2008)

- *The Delegated Administrator profile grants administrative access to a defined set of host groups and library servers.*
 - Users who belong to a Delegated Administrator role can use the VMM Administrator Console to modify the configuration of all virtual machines defined on any Hyper-V hosts that they control.
 - *The Self-Service User profile grants administrative access to a defined set of virtual machines through the Web-based Virtual Machine Manager Self-Service Portal.*
 - Self-service users cannot use the VMM 2008 console to manage virtual machine resources.
-
- ## ▶ NIC Management
- NICs are cheap. Segregate traffic to/from DMZs from each other and from the network
 - More expensive but cheaper in the long run compared to managing Vlans

Monitoring Systems

- ▶ Performance Monitoring can be done Using the performance counters included with Hyper-V and located on the VM Host.
 - Since the root has a full view of the system and controls the VM's it is also responsible for providing monitoring information via WMI and Performance Counters.
- ▶ Third party tools may also be used to monitor both hosts and virtual machines
 - SolarWinds
 - other

Monitoring Systems

- ▶ This section describes basic events/alarms that should be monitored:
 - *Overall health:*
 - Hyper-V Virtual Machine Health Summary
 - Hyper-V Hypervisor
 - *Processor:*
 - Processor
 - Hyper-V Hypervisor Logical Processor
 - %Guest Run
 - %Hypervisor Run Time
 - %Idle Run Time
 - %Total Run Time
 - Hyper-V Hypervisor Root Virtual Processor
 - Hyper-V Hypervisor Virtual Processor

Monitoring Systems– Cont.

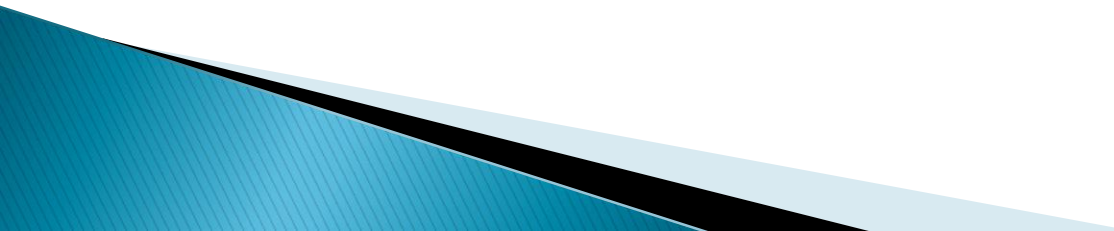
- ***Memory:***
 - Memory
 - Available Bytes
 - Pages /Sec
 - Hyper-V Hypervisor Partition
 - Hyper-V Root Partition
 - Hyper-V VM Vid Partition
- ***Storage:***
 - Physical Disk
 - Hyper-V Virtual Storage Device
 - Error Count
 - Flush Count
 - Read Bytes / Sec
 - Write Bytes / Sec
 - Read Count
 - Write Count
- ***Hyper-V Virtual IDE Controller***
 - Read Bytes / Sec
 - Write Bytes / Sec
 - Read Sectors / Sec
 - Write Sectors / Sec

Monitoring Hyper-V – Cont

- *Networking:*
 - Network Interface
 - Bytes Total / Sec
 - Offloaded Connections
 - Packets / Sec
 - Packets Outbound Errors
 - Packets Receive Errors
 - Hyper-V Virtual Switch
 - Bytes/Sec
 - Packets/Sec
 - Hyper-V Legacy Network Adapter
 - Bytes Dropped
 - Bytes Sent / Sec
 - Bytes Received / Sec
 - Hyper-V Virtual Network Adapter
 - Bytes / Sec
 - Packets / Sec

Virtual Machine Configuration

- VIRTUAL MACHINE CONFIGURATION PRACTICES

- *Apply consistent server naming conventions*
 - *Use proper OS type when building VMs (Standard, Enterprise, Datacenter).*
 - *Utilize Templates per OS type.*
 - *Use Synthetic Network Adapter, not Emulated Network Adapter (legacy).*
 - *VSs should be sized to the specific needs of the server and organization.*
 - *It is recommended that applications and databases be installed on separate partition and be properly sized.*
 - *VMs will typically be allocated 1 processor and a minimum 2 GB RAM; additional resources may be required for some applications or SQL database VMs*
 - *Understand and configure automatic power on options.*
- 

Integration with other MS Products

- SCVMM, SCOM, SCCM, DPM, Self-Service Portal
- ***System Center Virtual Machine Manager***
 - Utilizes a centralized management console to manage both Microsoft and VMWare virtual machines
 - Allows AD group based access to different groups of virtual servers.
 - Limit full access to SCVMM – Utilize user roles to assign appropriate access to users
 - SCVMM should run exclusively on its own server, no other software should be installed
 - Used to manage the Live Migration of virtuals between physical hosts
 - Utilize centralized Library for Templates, scripts, ISO images, etc.
 - Virtual Conversion Processes – P2V, V2V
- ***Microsoft System Center Data Protection Manager***
 - Utilize Backup and recovery of entire VMs
 - Offers host based backups (non CSV) or agent based (DPM 2010 will support backup of Cluster Shared Volumes (CSV))

Integration with other MS Products – Cont.

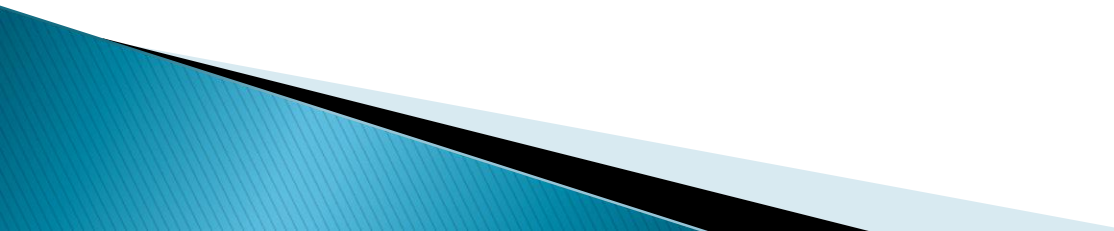
- ***Microsoft System Center Operations Manager***
 - Integrate with Windows Server to provide unified monitoring of physical servers and VMs
 - Utilize reporting components to gauge hardware usage
 - Integrates with the various System Center Products and provides usage data, reporting mechanisms, and tips for improving operations (Pro Tips)
- ***Microsoft System Center Configuration Manager***
 - Change and configuration management
- ***Self-Service Web Portal***
 - The VMM Self-Service Portal should be installed on a separate computer from the VMM server
 - Delegate VM provisioning utilizing the Self-Service Web Portal

Virtualization Hardware Requirements

- Servers

- ***Small Networks*** – Standard servers from major vendors. Determine if High Availability is needed for all/some/none. This will help determine if HA Clustering will be required as well as several other major components.
- ***Medium Networks*** – Standard servers or Blade Servers from major vendors – Perform a cost/benefit analysis to determine if a blade infrastructure fits the environment. Depending on the level of HA and recovery that is required, multisite replication may be necessary
- ***Large Networks*** – On enterprise class networks, multiple blade enclosures should be the standard. HA Clustering should be spread across enclosures in order to prevent downtime should a single enclosure fail. Depending on the level of HA and recovery that is required, multisite replication may be necessary

- CPU

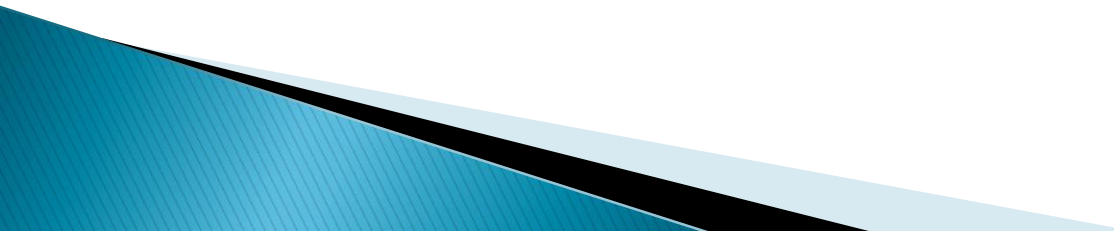
- At a minimum, each server should have dual quad core cpu's. Additional virtual server density will be attainable with additional cpu cores.
 - CPU's must support 64 bit environment, and be virtualization compliant
- 

Virtualization Hardware Requirements – Cont.

- RAM

- 64 gigs of RAM is recommended in order to maximize virtual server density on the host. Additional RAM is recommended in order to maximize the density of virtual servers.

- Storage

- ***Small Networks*** – If HA is not required, it is acceptable to utilize local storage for the virtual servers. It is a best practice to have a SAN and utilize the HA properties of the virtual environment
 - ***Medium Networks*** – Shared storage is recommended – Fiber channel (and subtypes), iSCSI, with dedicated switches, 15k RPM SAS drives, multipath configuration, monitoring. Sufficient space should be available for growth, backups, and additional space consumed by higher raid levels. Note: if clustering of virtual servers will be required, then iSCSI storage will be needed.
 - ***Large Networks*** – Enterprise class storage – Fiber channel (and subtypes), iSCSI, with dedicated switches, 15k RPM SAS drives, multipath configuration, monitoring. Sufficient space should be available for growth, backups, and additional space consumed by higher raid levels. Note: if clustering of virtual servers will be required, then iSCSI storage will be needed.
- 

Virtualization Hardware Requirements – Cont.

- Network

- ***Small Networks*** – Depending on the use of shared storage or HA clusters, a minimum of 4 gigabit nics should be available per server. More should be obtained where iSCSI shared storage is used to provide for multipath fault tolerance.
- ***Medium Networks*** – Blade environments – 6 gigabit ports per server, more may be needed depending on requirements. If standard servers are utilized, then 4–6 gigabit ports should be the minimum. Considerations for secured VLANs for various services (SQL, Email, etc.) or load balancing should be taken into account when building the infrastructure. Sufficient bandwidth should be available to the enclosures to allow for virtual server migration between enclosures, as well as the added network traffic of the virtual environment
- ***Large Networks*** – Blade environments – 6 gigabit ports per server, more may be needed depending on requirements. Considerations for secured VLANs for various services (SQL, Email, etc.) or load balancing should be taken into account when building the infrastructure. Sufficient bandwidth should be available to the enclosures to allow for virtual server migration between enclosures, as well as the added network traffic of the virtual environment

Operational Recovery

- Hyper-V Host Backups

- *Backup Hyper-V host to a media server.*

- This maintains host configuration info. This can be especially important for Clusters.
- This requires extra backups.

- *Prepare for a complete Hyper-V Host rebuild.*

- Often a complete rebuild is the quickest way to restore a Hyper-V host.
- Write down all settings. EX Networks, Physical settings, especially necessary for Clustering.

Operational Recovery – Cont.

- Hyper-V Virtual Machines Restores (Cont)

- *2 main backup methods*

- 1. Backup outside the Virtual Machine (VM) guest (Image-Level Backup) on the Hyper-V host. To do this the backup application must be compatible with the Hyper-V VSS writer. This requires the Integration services.
 - This is the preferred method.
 - This backs up also virtual machine configuration information such as drive, VM NIC, Memory, etc.
 - Restores are much easier.
 - You may not need to pay for backup agents within the individual VM.
 - One less application you will have to install within the VM.
 - Backs up virtual machine snapshots.
 - May not provide for application crash consistency.

Operational Recovery – Cont.

- **Hyper-V Virtual Machines Restores**
 - 2. Perform a backup from within the guest operating system of a VM (File-Level Backup). You use this method to backup data from inside the VM. Here you load the backup agent within the OS in each VM.
 - Needed for certain disk setups. EX Physical disks that are directly attached to a virtual machine and host-level backups of iSCSI volumes in guest VMs can't be backed up using the Hyper-V VSS writer.
 - Must document all VM configuration info for restore purposes.
 - Restores are more cumbersome.
 - More resource intensive on the host.
- No matter what your backup method is. It is imperative to test your backups with restores. Document your methods and locations of the restores.

Disaster Recovery – Cont.

Disaster Recovery (DR):

"Disaster recovery is a key component of business continuity. Natural disasters, malicious attacks, and even simple configuration problems like software conflicts can cripple services and applications until administrators resolve the problems and restore any backed up data. Leveraging the clustering capabilities of Windows Server 2008, Hyper-V now provides support for disaster recovery (DR) within IT environments and across data centers, using geographically dispersed clustering capabilities. Rapid and reliable disaster and business recovery helps ensure minimal data loss and powerful remote management capabilities." from <http://www.microsoft.com/windowsserver2008/en/us/hyperv-overview.aspx>

Your DR plan will often be dictated by your business requirements/objectives. This will often determine if you need a hot, warm, or cold site. How much data you can afford to lose and how long you can afford to be down will also help guide your site requirements.

Items to consider:

- If you need the fastest possible recovery you will need a hot site using technology such as Geo-Clustering. This will require some sort of 3rd party replication technology for VM replication.
- Make sure you have your backup media available.
- Make sure all appropriate hardware / network is available at disaster recovery location. EX servers, power, network, etc. Will you have to restore to like or different hardware? Processors can be an issue. Ideally with DR you will have like hardware on the other side.
- Make sure you test and document lessons learned.